FIREFLY HOST

Product Overview

Juniper Networks Firefly Host is a comprehensive virtualization security solution that includes integrated stateful inspection firewalling, intrusion detection, compliance monitoring and enforcement, as well as on-access and on-demand antivirus scanning. Purpose-built for virtualization, Firefly Host synchronizes with VMware vCenter to provide the highest levels of security and performance. Firefly Host delivers superior protection, throughput, scalability, automated deployment, operational efficiencies, and value for virtualized environments, enabling enterprises to maintain comparable security and regulatory compliance across physical and virtual networks.

Product Description

Juniper Networks® Firefly Host* is a comprehensive virtualization security solution that includes a high-performance, hypervisor-based stateful firewall, integrated intrusion detection system (IDS), virtualization-specific antivirus protection, and unrivaled scalability for managing multi-tenant cloud security. Firefly Host brings forward powerful features that offer layers of defenses and automated security as well as compliance enforcement within virtual networks and clouds. By leveraging virtual machine introspection (VM Introspection), coupled with Firefly Host's wide-ranging information about the virtual network environment, Firefly Host creates an extensive database of parameters by which security policies and compliance rules can be defined and enforced.

Firefly Host makes this rich data available in intuitive user interfaces that let administrators build the entire range of policies from corporate rules on global protocol handling (e.g., block Kazaa) to discrete regulatory compliance policies for how virtual machines should be configured (e.g., must have antivirus installed). Compliance assessment and security enforcement happen automatically and in lockstep with changes in the virtual environment. New virtual machines (VMs), for example, will be scanned and quarantined if out of compliance with policies in effect. The same applies to VMs whose "state" changes such that their security posture is weakened (e.g., antivirus protection is turned off). Firefly Host security operates from deep within the virtualization fabric as part of the hypervisor. Consequently, the software delivers unprecedented levels of security.

Security and compliance concerns are top of mind in virtualization and cloud deployments. Juniper's experience and innovative research in virtualization security have resulted in a powerful software suite capable of monitoring and protecting virtualized environments without negatively impacting performance. A hypervisor-based virtualization security approach, in combination with "x-ray" level knowledge of each virtual machine through VM Introspection, gives Firefly Host a unique vantage point in the virtualized fabric. Here, virtualization security can be applied efficiently and with context about the virtual environment and its state at any given moment.

*Formerly vGW Virtual Gateway

Firefly Host delivers total virtual data center protection and cloud security through visibility, protection, and compliance:

- **Visibility**—full view to all network traffic flowing between VMs. Complete VM and VM group inventory, including virtual network settings. Deep knowledge of VM state, including installed applications, operating systems, and patch level, through VM Introspection.
- **Protection**—a stateful firewall provides access control over all traffic via policies that include which ports, protocols, destination VMs, etc. should be blocked. Further, an integrated intrusion detection engine inspects packets for the presence of malware or malicious traffic and alerts as appropriate. Finally, virtualization-specific antivirus protections deliver highly efficient on-demand and on-access scanning of VM disks and files with the ability to quarantine infected entities.
- **Compliance**—enforcement of corporate and regulatory policies for the presence of required or banned applications via VM Introspection. Some practical applications of compliance enforcement, such as assurance of segregation of duties, ensure that VMs are assigned to the right trust zones inside the virtual environment. Pre-built compliance assessment is based on common industry best practices and leading regulatory standards. Firefly Host can also enforce compliance to a VM "gold" image with quarantine and alerting for non-compliance, thereby ensuring that deviations from the desired VM configuration do not create a security risk.

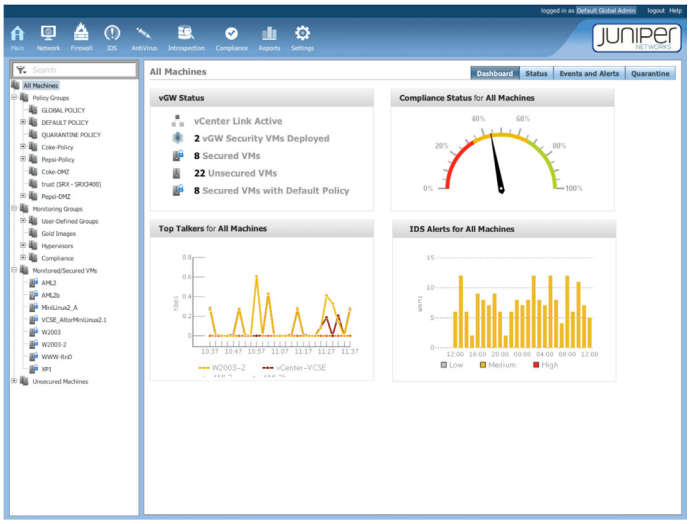
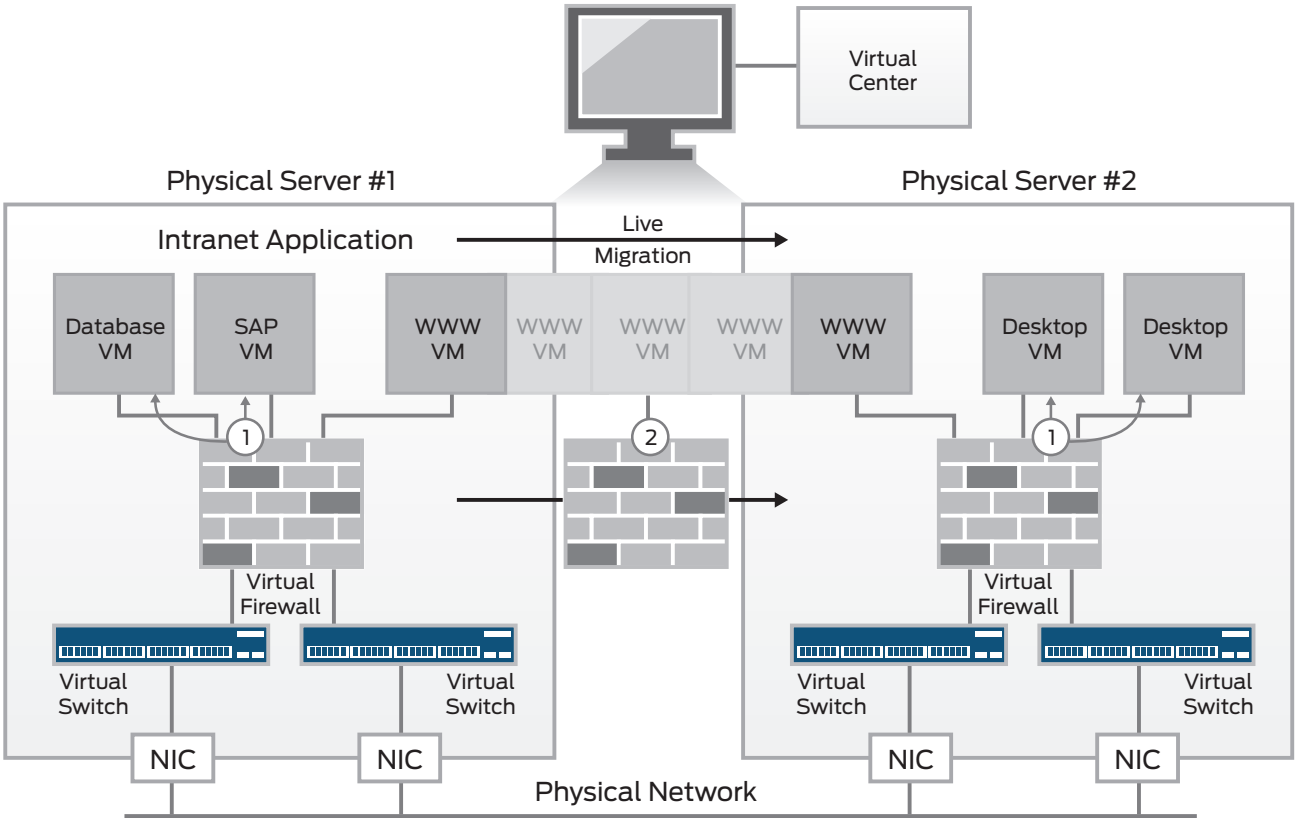


Figure 1: A dashboard view of virtual network security and compliance states.

Architecture and Key Components



Virtual Firewall

1. secure inter-VM communication, stopping infections.
2. Secure VMotion by "attaching" an enforceable policy to the migrating VM.

Figure 2: Firefly Host secures highly dynamic VMs through change and motion.

Features and Benefits

Virtualization has brought both economic benefits and new security concerns to enterprises. IT managers often hesitate to virtualize systems with sensitive data or take full advantage of VM live migration due to security worries. Among their concerns:

- Undetected and uncontained malware outbreaks or insider attacks in the virtual environment
- Lack of visibility into, or control of, traffic between VMs that never touches the physical network
- Inability to enforce policies that isolate VMs, prevent VM sprawl, or secure features like VMotion
- Virtualization compliance gaps and audit data holes
- Increasing network complexity and administrative burden caused by applying legacy VLAN or firewall technology to the virtual environment

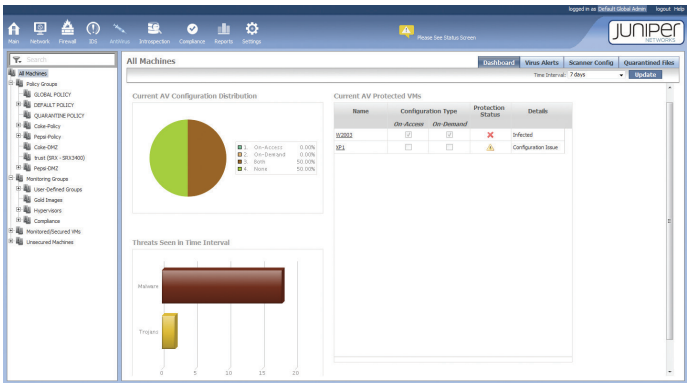


Figure 3: The Firefly Host antivirus allows for on-demand and on-access scanning of VMs and files.

By mitigating security risks in a cost-effective manner, Firefly Host enables enterprises to realize the full potential that virtualization technology has to offer.

Automated Deployment and Integration

Upon installation, the Firefly Host virtual appliance discovers all guest VMs through integration with VMware vCenter. Unlike using VLANs to isolate VMs, Juniper's solution is easy to maintain and readily scales as virtualization use grows and new virtual machines are added to the environment.

Automated VM Security

Firefly Host automates the application and enforcement of security rules. This is accomplished in two ways. First, Firefly Host allows for the creation of highly detailed security policies that dynamically combine desired conditions from a rich database of virtual infrastructure and VM information. The dynamic policy groups can then be associated with one or more VMs. When additional VMs are created, they can be automatically associated with known groups and policies by matching predefined criteria. Administration overhead is reduced by allowing a "build once, apply continuously" model to security policy definition and enforcement.

Cloud Security API

Juniper provides an XML-RPC programming interface that lets service providers and large enterprises customize and fully automate firewall provisioning lifecycle. This includes the ability to auto secure and "un" secure VMs without requiring administrator or tenant intervention. Users of the API can efficiently secure virtualization services for internal or external customers while ensuring strict isolation of customer VMs. Moreover, the API enables customers to integrate virtualization security into their existing VM provisioning and management systems.

Firewall Enforcement and Management for IPv6

Many organizations are now required—or even government-mandated—to support IPv6. Firefly Host offers firewall enforcement and management channel support for both IPv6 and IPv4 so that users can load either protocol on their VMs. This is critical for service providers who want to capitalize on the lead time to IPv6 adoption and ensure they can secure a mixed-mode IPv4/IPv6 network, as well as for any customer transitioning to IPv6 for more efficient routing and packet processing, multicast support, and other new and valuable services that enable faster content delivery.

Compliance

Firefly Host lets administrators, security managers, and compliance auditors define and report on the specific conditions (corporate and regulatory) that constitute compliant operation in their environments. The Firefly Host user interface allows for the building of custom whitelists (desired configurations) and blacklists (unwanted conditions). Firefly Host continuously monitors all VMs, including all ESX/ESXi hosts and VMs (even newly created ones), to report on the overall compliance posture of the virtual environment. Virtual data center and cloud administrators can see their aggregate compliance posture at a glance, and drill down on each VM to identify the exact condition that has triggered a noncompliance alert (e.g., VM in virtual port group, or missing important software like VMware tools or backup agents).

High Availability

Using redundant system components, Firefly Host provides mission critical reliability. Easily deployed standby systems can immediately take over if any of the primary systems fail, ensuring uninterrupted VM connectivity, security, and policy enforcement.

High-Performance, Hypervisor-Resident Firewall

By processing inspections in the VMware hypervisor kernel, Firefly Host provides more than 10 times the throughput of older, bridge mode firewalls running in virtual environments. This optimized innovation can increase secured VMs per host while eliminating network reconfigurations. Firewall protection is continuous as VMs move from host to host using VMotion. Firefly Host keeps the "live" in live migration by maintaining open connections and security throughout the event.

Integrated Intrusion Detection

The Firefly Host intrusion detection system (IDS) is fully integrated with the virtual firewall. Rule-based IDS enables selective deep packet inspection of allowed traffic for malware suppression, maximizing the host resources available for VMs. Alerts are generated automatically and stakeholders receive relevant reports. Further, Firefly Host IDS identifies the alert source and provides the mechanism for shutdown.

Integrated Antivirus

Virtualization-specific antivirus adds another layer of defense against malware (such as viruses, worms, and spyware) with minimal impact on VM memory and disk. The Firefly Host antivirus engine provides optional on-access and on-demand scanning so that administrators can either choose to scan files in real time or use the completely agent-less offline approach. With numerous options for when and what to scan, organizations can optimize their antivirus scanning mechanisms for performance in the most cost-effective manner by obviating the need to buy licenses for all VMs or run CPU-intensive applications on VM hosts.

Intuitive and Highly Scalable Central Management

The web-based central management console displays real-time views of each virtual machine's operating and security status at a glance. This offers a simple, familiar interface for defining rules and managing policies to support role-based administration, enabling separation of duties.

Multi-Center

The Multi-Center feature allows Firefly Host to import virtualization information from multiple and even geographically disparate VMware vCenters. Firefly Host administrators have the benefit of a singular logical view of the virtualized network, making the configuration of security policies faster and less prone to error. This unique synchronization capability makes Firefly Host the top choice for global organizations and service providers with ever growing virtualized environments that require cost-effective security at scale.

Split-Center

Split-Center is available in cases where large-scale virtualized environments—especially multi-tenant ones—require segregation of a single security management platform into parts that are consistent with unique security policies per tenant. Split-Center allows for logical segmentation of the data contained in one VMware vCenter into what are effectively seen as multiple "independently managed" Firefly Host centers to improve resource isolation for cloud services/multi-tenancy. Based on the granularity of control they require, administrators can set up management domains that consist of: the entire vCenter; multiple data centers within the vCenter; or multiple clusters of VM hosts within the vCenter.

Logging, Reporting, and Alerts

System logging output gives security event management systems insight into virtual network activity. Administrators can print reports of historical VM traffic data and configure SNMP traps to alert them to selected events. Those events can then be sent via system logs to third-party security products like those specializing in Security Information and Event Management (SIEM) such as Juniper Networks STRM Series Security Threat Response Managers. These products can synthesize Firefly Host log and event information from the virtualized data center with events from other parts of the network in order to get a holistic picture of the entire data center and its security posture.

Hypervisor Compliance Monitoring

Firefly Host compliance checks extend to the maintenance of the hypervisor and its security posture. The Firefly Host compliance engine can be configured to generate alerts to stakeholders when conditions change on the ESX host such that their impact is understood to increase risk. This type of continuous monitoring ensures that changes to the hypervisor or ESX host configuration and access rights get additional scrutiny and aims at mitigating exposure through erroneous or improper virtual infrastructure administrator action.

VM Introspection

VM Introspection is a groundbreaking approach, analogous to an "x-ray" of VMs and the virtual environment from the hypervisor. VM Introspection enables information gathering about Windows- and Linux-based VMs, the security of the virtual network, and virtual environment settings—without the use of agents. The ability of malware to disable or hide from security agents is a classic unresolved security problem that has plagued the security industry for decades. Not only does Firefly Host incorporate VM Introspection as part of its security policy definition and enforcement mechanism, but Firefly Host also combines VM Introspection and antivirus features to offer an innovative new approach to leveraging the hypervisor for an uncompromised x-ray inspection of VMs, where malware literally has nowhere to hide.

By amassing information about the kinds of applications and services running on VMs, Firefly Host sustains deep knowledge about the internal security state of each virtual system. This information is then made available through the Firefly Host point-and-click dynamic policy editor, so that rules can easily be built to enforce a desired VM security posture.

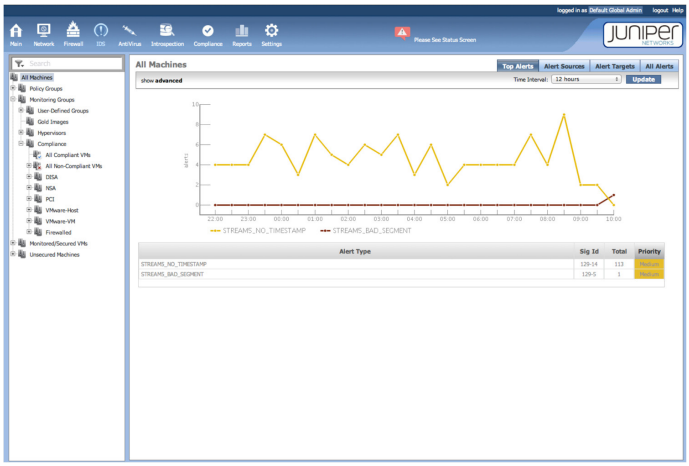


Figure 4: Firefly Host IDS enables deep packet inspection of traffic for malware suppression.

Specifications

Firefly Host Security VM

- Operating System Virtual Appliance
- Memory: 512 MB
- Disk Space: 2.0 GB

Security Design for Firefly Host

- Operating System Virtual Appliance
- Memory: 2 GB
- Disk Space: 11 GB

VMware vSphere 4.x (ESX/ESXi), vSphere 5.x

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services**.

Ordering Information

For more information about Juniper Networks Firefly Host, please go to **www.juniper.net** or contact the nearest Juniper Networks sales representative.

Model Number	Description
VGW-CENTER-1	Central management center
VGW-SVM-ADD-2	Security VM license for 2 CPU sockets
VGW-SVM-ADD-10	Security VM license for 10 CPU sockets
VGW-SVM-ADD-20	Security VM license for 20 CPU sockets
VGW-SVM-ADD-50	Security VM license for 50 CPU sockets
VGW-SVM-ADD-100	Security VM license for 100 CPU sockets
VGW-HA-ADD-2	High availability license for 2 CPU sockets
VGW-HA-ADD-10	High availability license for 10 CPU sockets
VGW-HA-ADD-20	High availability license for 20 CPU sockets
VGW-HA-ADD-50	High availability license for 50 CPU sockets
VGW-HA-ADD-100	High availability license for 100 CPU sockets
VGW-IDS-ADD-2	One year IDS subscription for 2 CPU sockets
VGW-IDS-ADD-10	One year IDS subscription for 10 CPU sockets
VGW-IDS-ADD-20	One year IDS subscription for 20 CPU sockets
VGW-IDS-ADD-50	One year IDS subscription for 50 CPU sockets
VGW-IDS-ADD-100	One year IDS subscription for 100 CPU sockets
VGW-AV-ADD-2	One year antivirus subscription for 2 CPU sockets
VGW-AV-ADD-10	One year antivirus subscription for 10 CPU sockets
VGW-AV-ADD-20	One year antivirus subscription for 20 CPU sockets
VGW-AV-ADD-50	One year antivirus subscription for 50 CPU sockets
VGW-AV-ADD-100	One year antivirus subscription for 100 CPU sockets

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at +1-866-298-6428 or authorized reseller.

1000363-008-EN Dec 2013

Printed on recycled paper